

⑥(7) 文献

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-293717

(43)Date of publication of application : 20.10.2000

(51)Int.Cl.

G07B 15/00

G06F 15/00

G06K 17/00

(21)Application number : 11-102898

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 09.04.1999

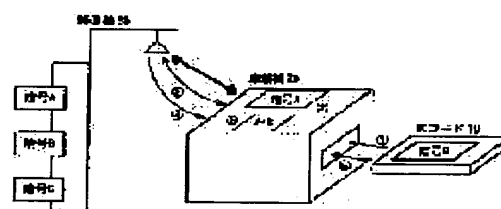
(72)Inventor : KAWASAKI AKIHISA

## (54) SYSTEM AND METHOD FOR AUTHENTICATION

(57)Abstract:

**PROBLEM TO BE SOLVED:** To make the rightfulness of access to be confirmed between an on-vehicle machine and an IC card inserted into the on-vehicle machine when the IC card is an authorized card even when the IC card has a different cipher.

**SOLUTION:** An authentication system is constituted to make two-step authentication in such a way that a road-side machine 30 confirms an on-vehicle machine 20 and the machine 20 confirms an IC card 10 inserted into the machine 20. In addition, the on-vehicle machine 20 is constituted to be able to confirm the IC card 10 as an authorized card by making data communication with the road-side machine 30 even when the cipher of the card 10 is not coincident with that of the machine 20.



## LEGAL STATUS

[Date of request for examination]

06.12.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the

examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3091450

[Date of registration]

21.07.2000

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-293717  
(P2000-293717A)

(43) 公開日 平成12年10月20日 (2000. 10. 20)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト* (参考)
G 0 7 B 15/00	5 1 0	G 0 7 B 15/00	L 3 E 0 2 7
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	5 1 0 5 B 0 5 8
G 0 6 K 17/00		G 0 6 K 17/00	3 3 0 B 5 B 0 8 5
			T

審査請求 有 請求項の数 6 O L (全 8 頁)

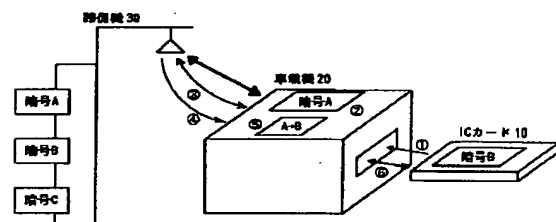
(21) 出願番号	特願平11-102898	(71) 出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22) 出願日	平成11年4月9日 (1999. 4. 9)	(72) 発明者	川崎 晃久 神奈川県横浜市港北区綱島東四丁目3番1号 松下通信工業株式会社内
		(74) 代理人	100099254 弁理士 役 昌明 (外3名)
		Fターム(参考)	3E027 EA01 EC06 EC08 EC10 5B058 CA15 KA33 KA35 YA01 5B085 AE03 AE12 AE23

(54) 【発明の名称】 認証システム及び認証方法

(57) 【要約】

【課題】 異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しうる認証システム及び認証方法を提供する。

【解決手段】 路側機30は車載機20を認証し、車載機20はICカード10を認証するという2段階認証を行なう認証システムにおいて、車載機20の暗号と一致しないICカード10が車載機20に挿入されたとしても、車載機20と路側機30との間のデータ通信によって車載機20がICカード10をオーソライズされたICカードであることを認証できるようにする。



## 【特許請求の範囲】

【請求項1】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入されたとしても、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しうるようにすることを特徴とする認証システム。

【請求項2】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入されたとしても、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しうるようにすることを特徴とする認証方法。

【請求項3】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機は、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記ICカードとの間で相互認証を実施するようにしたことを特徴とする認証システム。

【請求項4】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機は、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記ICカードとの間で相互認証を実施するようにしたことを特徴とする認証方法。

【請求項5】 請求項3記載の認証システムにおいて、前記車載機で行なった上書きに基づく前記ICカードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記ICカードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項3記載の認証システム。

【請求項6】 請求項4記載の認証方法において、前記

車載機で行なった上書きに基づく前記ICカードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記ICカードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項4記載の認証方法。

【請求項7】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信の際に前記車載機は挿入されたICカードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しうるようにすることを特徴とする認証システム。

【請求項8】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信の際に前記車載機は挿入されたICカードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しうるようにすることを特徴とする認証方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は認証システム及び認証方法に関し、特に、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しうるようにしたものである。

## 【0002】

【従来の技術】図2は従来の認証システム全体の構成を統括的に説明するものである。図2において、認証システム全体の構成は、ICカード1と、車載機2と、路側機3とから構成される。そして、路側機3は、図示されていない中央処理装置とETC（自動料金収受システム）に関するデータのやりとりを実施するようになっている。

【0003】車載機2は、車載機2と路側機3間の相互認証動作と、車載機2とICカード1間の相互認証動作を行なうために、ICカード1及び路側機3と共通する暗号を有するようにされている。

【0004】次に従来の認証システムの動作について図2を参照しながら説明する。図2において、

① ICカード1を車載機2のカードスロット部に挿入す

る。車載機2に挿入されたICカード1は、車載機2との間で相互認証を行なう。このとき、車載機2とICカード1に格納されている暗号が暗号Aで共通しているので認証は成立し、ICカード1は車載機2を正当とみなせる。

【0005】②車載機2から見てICカード1を正当と見なせるので、暗号一致を検出する。

【0006】③暗号一致を検出した車載機2は、路側機3との通信を行なって相互認証を行なう。この場合、車載機2と路側機3とは暗号Aで共通しているので、相互に正当な車載機2、路側機3であることを確認することができる。これによりETC（自動料金収受システム）に関するデータのやりとりを実施することができるようになる。

【0007】上記においてももしもICカード1に暗号Bが格納されていた場合には、車載機2及び路側機3には暗号Aだけ格納されているだけなので、車載機2と路側機3との間では相互認証が行なえても、車載機2とICカード1の間では相互認証を行なうことはできない。

【0008】

【発明が解決しようとする課題】このように従来のETC（自動料金収受システム）等で実施されている認証システムは、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムであり、その認証システムに共通する暗号を有するようにしているものであり、異なる暗号を有する場合にはETCにおける認証はできないという課題を有していた。

【0009】そこで、本発明は、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しようようにする認証システム及び認証方法を提供することを目的とするものである。

【0010】

【課題を解決するための手段】本発明による認証システムは、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入されたとしても、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しようようにすることを特徴とする。

【0011】このような構成とすることにより、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しようという優れた効果を有する。

【0012】

【発明の実施の形態】本発明の請求項1記載の発明は、路側機は車載機を認証し、車載機はICカードを認証す

るという2段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入されたとしても、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しようようにすることを特徴とする認証システムとしたものであり、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しようという作用を有する。

【0013】また、請求項2記載の発明は、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入されたとしても、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しようようにすることを特徴とする認証方法としたものであり、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しようという作用を有する。

【0014】また、請求項3記載の発明は、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機は、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に書き換えてそれを新たな暗号方式として前記ICカードとの間で相互認証を実施するようにしたことを特徴とする認証システムとしたものであり、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しようという作用を有する。

【0015】また、請求項4記載の発明は、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機は、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に書き換えてそれを新たな暗号方式として前記ICカードとの間で相互認証を実施するようにしたことを特徴とする認証方法としたものであり、異な

る暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証するという作用を有する。

【0016】また、請求項5記載の発明は、請求項3記載の認証システムにおいて、前記車載機で行なった上書きに基づく前記ICカードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記ICカードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項3記載の認証システムとしたものであり、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証するという作用を有する。

【0017】また、請求項6記載の発明は、請求項4記載の認証方法において、前記車載機で行なった上書きに基づく前記ICカードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記ICカードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項4記載の認証方法としたものであり、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証するという作用を有する。

【0018】また、請求項7記載の発明は、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信の際に前記車載機は挿入されたICカードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しようようにすることを特徴とする認証システムとしたものであり、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証するという作用を有する。

【0019】また、請求項8記載の発明は、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信

の際に前記車載機は挿入されたICカードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しようようにすることを特徴とする認証方法としたものであり、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しようという作用を有する。

【0020】以下、本発明の実施の形態について、図面を使用して説明する。

【0021】図1は認証システム全体の構成を統括的に説明するものである。図1において、認証システム全体の構成は、ICカード10と、車載機20と、路側機30とから構成される。そして、路側機30には、図示されていない中央処理装置によってあらかじめシステム間でやり取りされるであろうすべての暗号方式、この例では暗号A、暗号Bおよび暗号Cが内部の記憶装置に記憶されるようにしてある。

【0022】また、ICカード10には、特定の暗号方式(以下、暗号という)だけを持つように権限を委任されたICカード発行者によって設定される。

【0023】また、車載機20は、車載機20と路側機30間の相互認証動作と、車載機20とICカード10間の相互認証動作とを行なうために、路側機30とのデータ転送によって暗号を変更・保持するようにされている。

【0024】次に本発明の認証システムの動作について図1を参照しながら説明する。図1において、

①ICカード10を車載機20のカードスロット部に挿入する。車載機20に挿入されたICカード10は、車載機20との間で相互認証を行なう。このとき、車載機20とICカード10に格納されている暗号が一致すれば認証は成立し車載機20はICカード10を正当と見なせるし、ICカード10は車載機20を正当とみなせる。(図2の従来例を参照されたい。)

【0025】しかしながら、車載機20とICカード10に格納されている暗号が一致しない場合、すなわち図1のようにICカード10に暗号Bが格納されている場合に、車載機20には暗号Aが格納されている場合には、

②車載機20では認証NGとともに、暗号不一致を検出する。

【0026】③暗号不一致を検出した車載機20は、路側機30との通信を行なったときに相互認証を行なう。この場合、車載機20には暗号Aが格納されていることと、路側機30はすべての暗号A～Cを保持しているので、相互に正当な車載機20、路側機30であることを確認することができ、ここで確認がなされたならば、

④車載機20は路側機30に、車載機20とICカード10との間で暗号不一致の判定情報を送り、此の情報を受けた路側機30は車載機20に暗号Bを送出する。

【0027】⑤暗号Bを受け取った車載機20では暗号Bを暗号Aに上書きする。

【0028】⑥上書きを完了した車載機20はICカード10との間で暗号Bにより相互認証を再度行なうことで、ICカード10と車載機20との間の認証を成立させる。

【0029】この例の場合には、暗号Bで認証を成立させることができたが、この段階でも認証が不成立であれば、再度上記③～⑥を繰り返すようにすることでかならず認証を成立させることができる。

【0030】なお、上記④においては、車載機20とICカード10との間での暗号不一致の判定情報を車載機20から路側機30に送ったが、この不一致の判定情報だけでなく、ICカードにどの暗号が組み込まれているかの情報を併せて送るようにしても良いことは勿論である。この場合には、上記のように認証が不成立の場合における繰り返しルーチン③～⑥を経ずに直ちに路側機30から車載機20に的確な暗号を送信することができる。

【0031】以上により本発明の実施の形態によれば、車載機の暗号と一致しないICカードが車載機に挿入されたとしても、車載機が路側機を通過することによる車載機と路側機との間のデータ転送によって車載機がICカードを認証することができるようになる。

【0032】

\*

\*【発明の効果】以上説明したように本発明の認証システムおよび認証方法は、路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入されたとしても、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しうるようにすることを特徴とする。

【0033】このような構成とすることにより、異なる暗号を有するICカードを車載機に挿入してもそれがオーソライズされたICカードである場合には、車載機とICカードとの間でアクセスの正当性を認証しうるという優れた効果を有する。

【図面の簡単な説明】

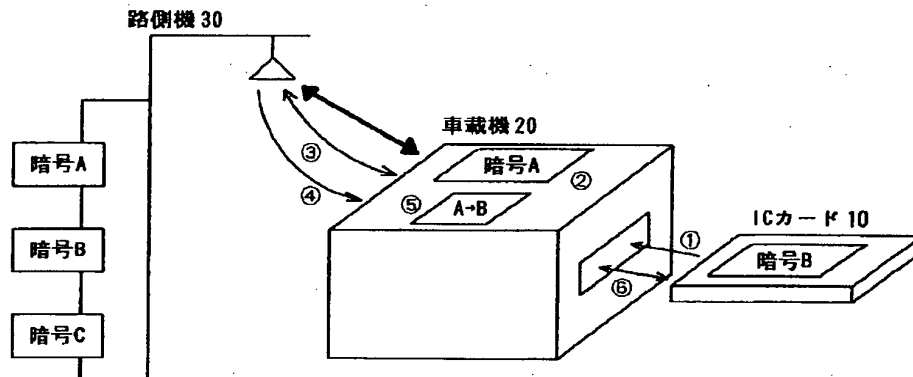
【図1】本発明の実施形態に係る認証システム全体の構成を統括的に示したブロック図、

【図2】従来の認証システム全体の構成を統括的に示したブロック図である。

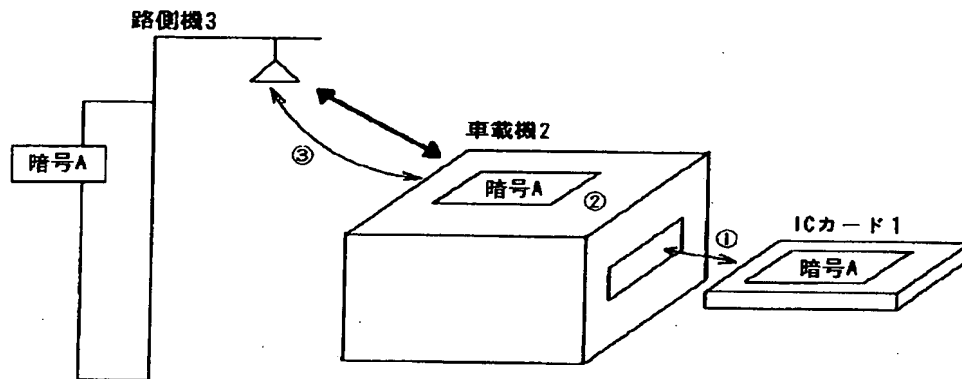
【符号の説明】

- 1、10 ICカード
- 2、20 車載機
- 3、30 路側機

【図1】



【図2】



## 【手続補正書】

【提出日】平成12年5月8日(2000.5.8)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機は、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記ICカードとの間で相互認証を実施するようにしたことを特徴とする認証システム。

【請求項2】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機は、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記ICカードとの間で相互認証を実施するようにしたことを特徴とする認証方法。

【請求項3】 請求項1記載の認証システムにおいて、

前記車載機で行なった上書きに基づく前記ICカードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記ICカードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項1記載の認証システム。

【請求項4】 請求項2記載の認証方法において、前記車載機で行なった上書きに基づく前記ICカードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記ICカードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項2記載の認証方法。

【請求項5】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信の際に前記車載機は挿入されたICカードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ICカードをオーソライズされたICカードであることを認証しうるようにすることを特徴とする認証システム。

【請求項6】 路側機は車載機を認証し、車載機はICカードを認証するという2段階認証を行なう認証方法において、前記車載機の暗号と一致しない前記ICカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信の際に前記車載機は挿入され

た IC カードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記 IC カードをオーソライズされた IC カードであることを認証しうるようにすることを特徴とする認証方法。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正内容】

【0010】

【課題を解決するための手段】本発明の認証システムは、路側機は車載機を認証し、車載機は IC カードを認証するという 2 段階認証を行なう認証システムにおいて、前記車載機は、前記車載機の暗号と一致しない前記 IC カードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記 IC カードとの間で相互認証を実施するようにしたことを特徴とする。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正内容】

【0012】

【発明の実施の形態】本発明の請求項 1 記載の発明は、路側機は車載機を認証し、車載機は IC カードを認証するという 2 段階認証を行なう認証システムにおいて、前記車載機は、前記車載機の暗号と一致しない前記 IC カードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記 IC カードとの間で相互認証を実施するようにしたことを特徴とする認証システムとしたものであり、異なる暗号を有する IC カードを車載機に挿入してもそれがオーソライズされた IC カードである場合には、車載機と IC カードとの間でアクセスの正当性を認証しうるという作用を有する。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正内容】

【0013】また、請求項 2 記載の発明は、路側機は車載機を認証し、車載機は IC カードを認証するという 2 段階認証を行なう認証方法において、前記車載機は、前記車載機の暗号と一致しない前記 IC カードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記 IC カードとの間で相互認証を実施するようにしたことを特徴とする認証方法としたものであり、異なる暗号を有する IC カードを車載機に挿入してもそれがオーソライズされた IC カードである場合には、車載機と IC カードとの間でアクセスの正当性を認証しうるという作用を有する。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正内容】

【0014】また、請求項 3 記載の発明は、請求項 1 記載の認証システムにおいて、前記車載機で行なった上書きに基づく前記 IC カードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記 IC カードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項 1 記載の認証システムとしたものであり、異なる暗号を有する IC カードを車載機に挿入してもそれがオーソライズされた IC カードである場合には、車載機と IC カードとの間でアクセスの正当性を認証しうるという作用を有する。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

【補正内容】

【0015】また、請求項 4 記載の発明は、請求項 2 記載の認証方法において、前記車載機で行なった上書きに基づく前記 IC カードとの相互認証に失敗した場合には、前記路側機に暗号不一致であるとの判定情報を前記路側機に再度送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から再度受け取ると、前記車載機に現在と異なる暗号方式を送出し、以下前記 IC カードとの間で相互認証が成立するまでこれを繰り返すことを特徴とする請求項 2 記載の認証方法としたものであり、異なる暗号を有する IC カードを車載機に挿入してもそれがオーソライズされた IC カードである場合に



は、車載機とＩＣカードとの間でアクセスの正当性を認証するという作用を有する。

【手続補正７】

【補正対象書類名】明細書

【補正対象項目名】００１６

【補正方法】変更

【補正内容】

【００１６】また、請求項５記載の発明は、路側機は車載機を認証し、車載機はＩＣカードを認証するという２段階認証を行なう認証システムにおいて、前記車載機の暗号と一致しない前記ＩＣカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信の際に前記車載機は挿入されたＩＣカードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車載機と前記路側機との間のデータ通信によって前記車載機が前記ＩＣカードをオーソライズされたＩＣカードであることを認証しうるようにすることを特徴とする認証システムとしたものであり、異なる暗号を有するＩＣカードを車載機に挿入してもそれがオーソライズされたＩＣカードである場合には、車載機とＩＣカードとの間でアクセスの正当性を認証しうるとい作用を有する。

【手続補正８】

【補正対象書類名】明細書

【補正対象項目名】００１７

【補正方法】変更

【補正内容】

【００１７】また、請求項６記載の発明は、路側機は車載機を認証し、車載機はＩＣカードを認証するという２段階認証を行なう認証方法において、前記車載機の暗号と一致しない前記ＩＣカードが前記車載機に挿入された場合には、前記車載機と前記路側機との間のデータ通信の際に前記車載機は挿入されたＩＣカードの暗号方式も併せて前記路側機にデータ通信するようにして、前記車

載機と前記路側機との間のデータ通信によって前記車載機が前記ＩＣカードをオーソライズされたＩＣカードであることを認証しうるようにすることを特徴とする認証方法としたものであり、異なる暗号を有するＩＣカードを車載機に挿入してもそれがオーソライズされたＩＣカードである場合には、車載機とＩＣカードとの間でアクセスの正当性を認証しうるとい作用を有する。

【手続補正９】

【補正対象書類名】明細書

【補正対象項目名】００１８

【補正方法】削除

【手続補正１０】

【補正対象書類名】明細書

【補正対象項目名】００１９

【補正方法】削除

【手続補正１１】

【補正対象書類名】明細書

【補正対象項目名】００３２

【補正方法】変更

【補正内容】

【００３２】

【発明の効果】以上説明したように本発明の認証システムおよび認証方法は、路側機は車載機を認証し、車載機はＩＣカードを認証するという２段階認証を行なう認証システムにおいて、前記車載機は、前記車載機の暗号と一致しない前記ＩＣカードが前記車載機に挿入された場合には、前記車載機は前記路側機に暗号不一致であるとの判定情報を前記路側機に送出し、前記路側機は、暗号不一致であるとの判定情報を前記車載機から受け取ると、前記車載機に現在と異なる暗号方式を送出し、それを受け取った前記車載機は現在まで使用していた暗号方式に上書きしてそれを新たな暗号方式として前記ＩＣカードとの間で相互認証を実施するようにしたことを特徴とする。